CYBERSECURITY: a growing risk for supply chain risk management

Mark Weatherford
SVP & Chief Cybersecurity Strategist, vArmour

Amateurs study cryptography;
Professionals study economics.

- Allan Schiffman, July 2, 2004

Three Maxim's of Cybersecurity

1. People, Process and Technology
2. Confidentiality, Integrity and Availability (CIA)
3. Cyber Risk = Threat x Vulnerability x Consequence

"A growing set of threat actors are now capable of using cyber operations to remotely access traditional Intelligence targets, as well as a broader set of US targets including critical infrastructure supply chains."

- William Evanina, National Counter Intelligence Center in a testimony to Senate Intelligence Committee on Intelligence, May 15, 2018

"The greatest transfer of wealth in human history." *

- Cyber crime
- Cyber deterrence
- Cyber espionage
- Cyber sabotage
- Cyber terrorism
- Cyber warfare
- Cyber-enabled information warfare
- Cyber-enabled economic warfare

* General Keith Alexander, NSA

In no other arena are civilian government or private organizations expected to do battle with the likes of:

Global Nation States

- Cyber espionage and IP theft
- Economic and competitive intelligence

International organized crime

- Customer and credit card account manipulation
- Harvesting PII for identity theft

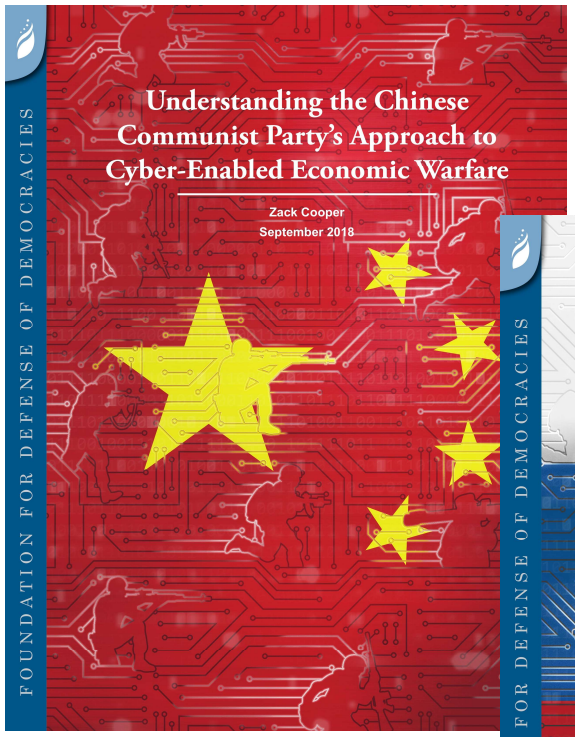
Terrorists

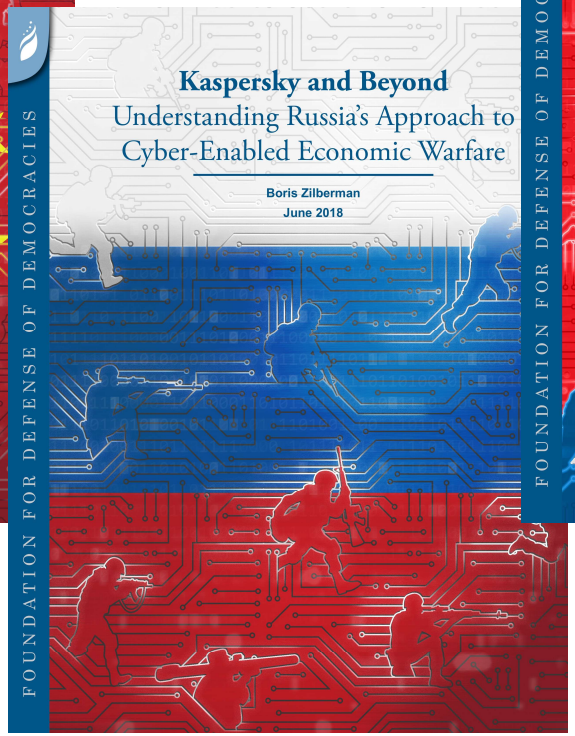
- Targeting critical infrastructures
- Maximum lethal impact to society

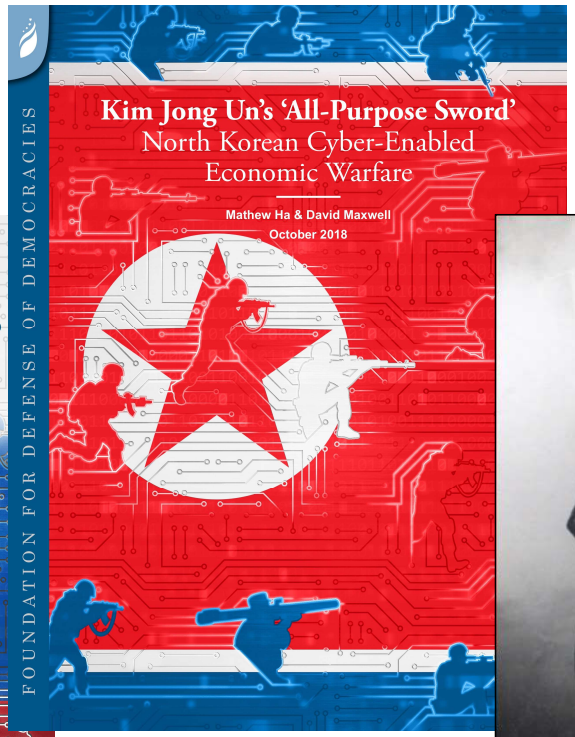
Hacktivists

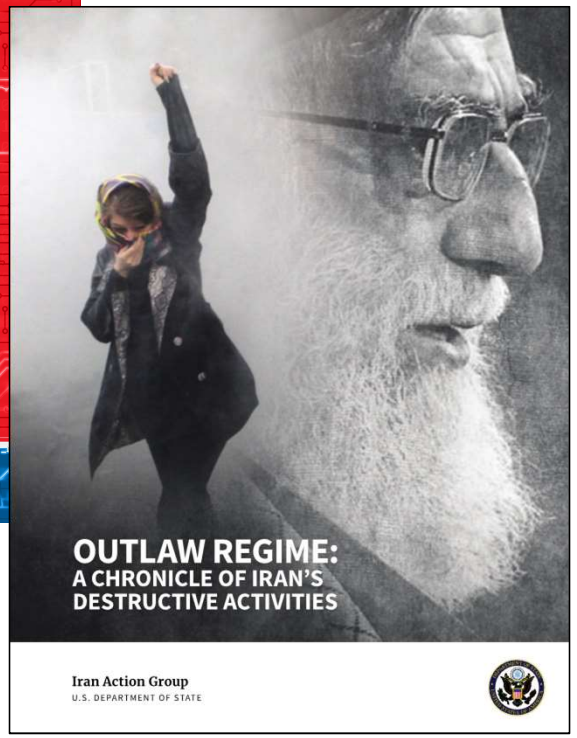
- Political hacktivism and hacking for the *Lulz*
- Cyber-civil disobedience

The big four nation state actors









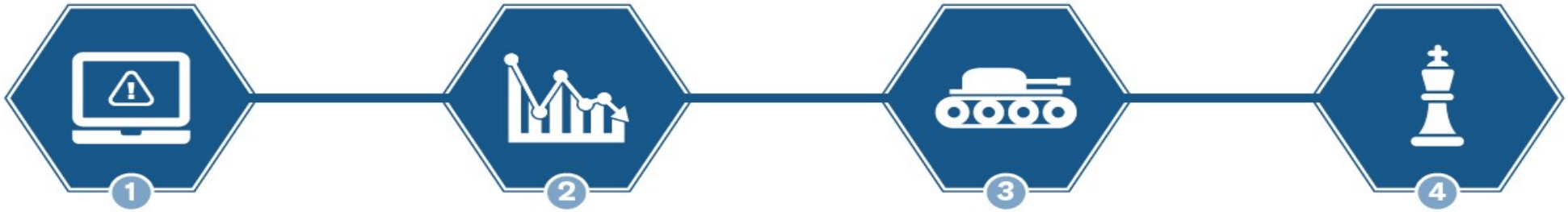
Cyber enablement has changed everything

- Economic warfare has evolved in the face of an exponentially growing digital supply chain
- Cyber-enabled supply chain attacks can now result in *vastly disproportionate economic harm* compared to the minimal resources required to execute the attack

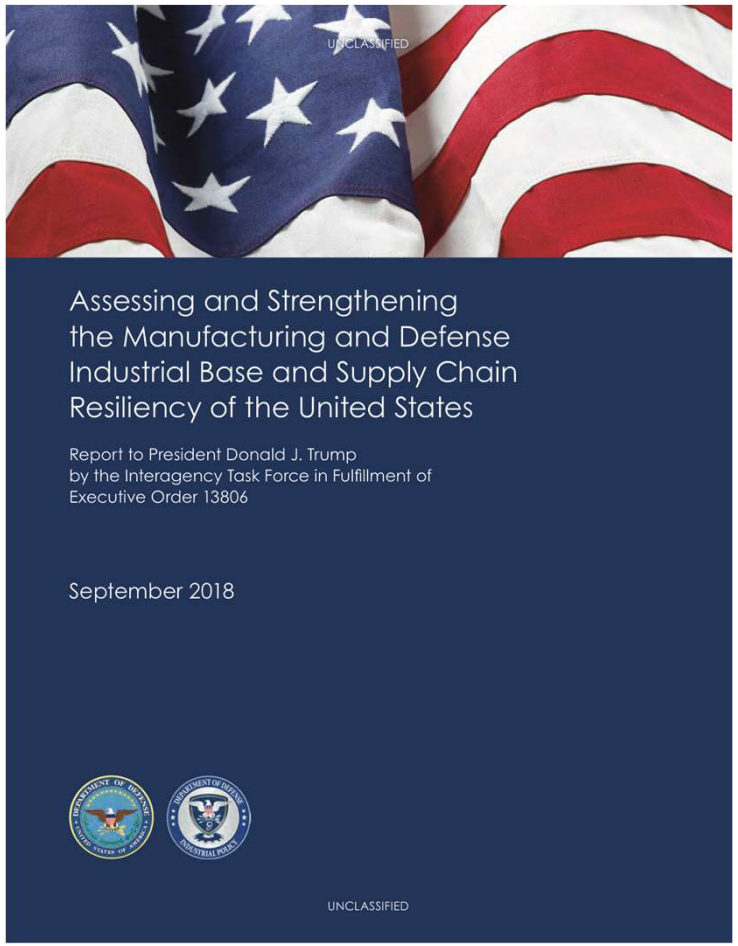
Cyber-Enabled Economic Warfare (CEEW)

"A hostile strategy involving attack(s) against a nation using cyber technology with the intent to weaken its economy and thereby reduce its political and military power."

An attack, or collection of attacks, constitutes CEEW if it meets the following four requirements:



1. It must be cyber-enabled
2. It must cause, or be intended to cause, economic harm
3. The economic damage must be significant enough to potentially degrade national security capabilities
4. The attack(s) must be motivated by the strategic intent to erode national security capabilities



Beijing "is increasingly dominating downstream value-added materials processing and associated manufacturing supply chains, both in China and increasingly in other countries."

- Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, September 2018

Supply Chain Cybersecurity is a subset of supply chain risk management and is focused on the management of cybersecurity requirements for IT systems, software, and networks, which are driven by threats such as cyber-terrorism, malware, data theft, and the advanced persistent threats (APT).

Typical supply chain cybersecurity activities for minimizing risks include *buying only from trusted vendors, disconnecting critical machines from the Internet and outside networks, and educating users on the threats and protective measures they can take.*

- Wikipedia

Supply chains are the backbone of today's global economy and any organization
- government or private –
that relies on an external supply chain to accomplish their business goals is a player in supply chain risk management

The business eco-system is complex

84 Days
Supply of F150's after fire halted production at Ford supplier

306,000
The number of direct (Tier 1) dairy farmers to Nestle

10 minutes
Warehouse fire that cost Ericsson $2.34B and its place in the cell phone market

175
Number of parts GM relied on from a single supplier when they went bankrupt

100,000+
Worldwide pool of Walmart direct (Tier 1) suppliers

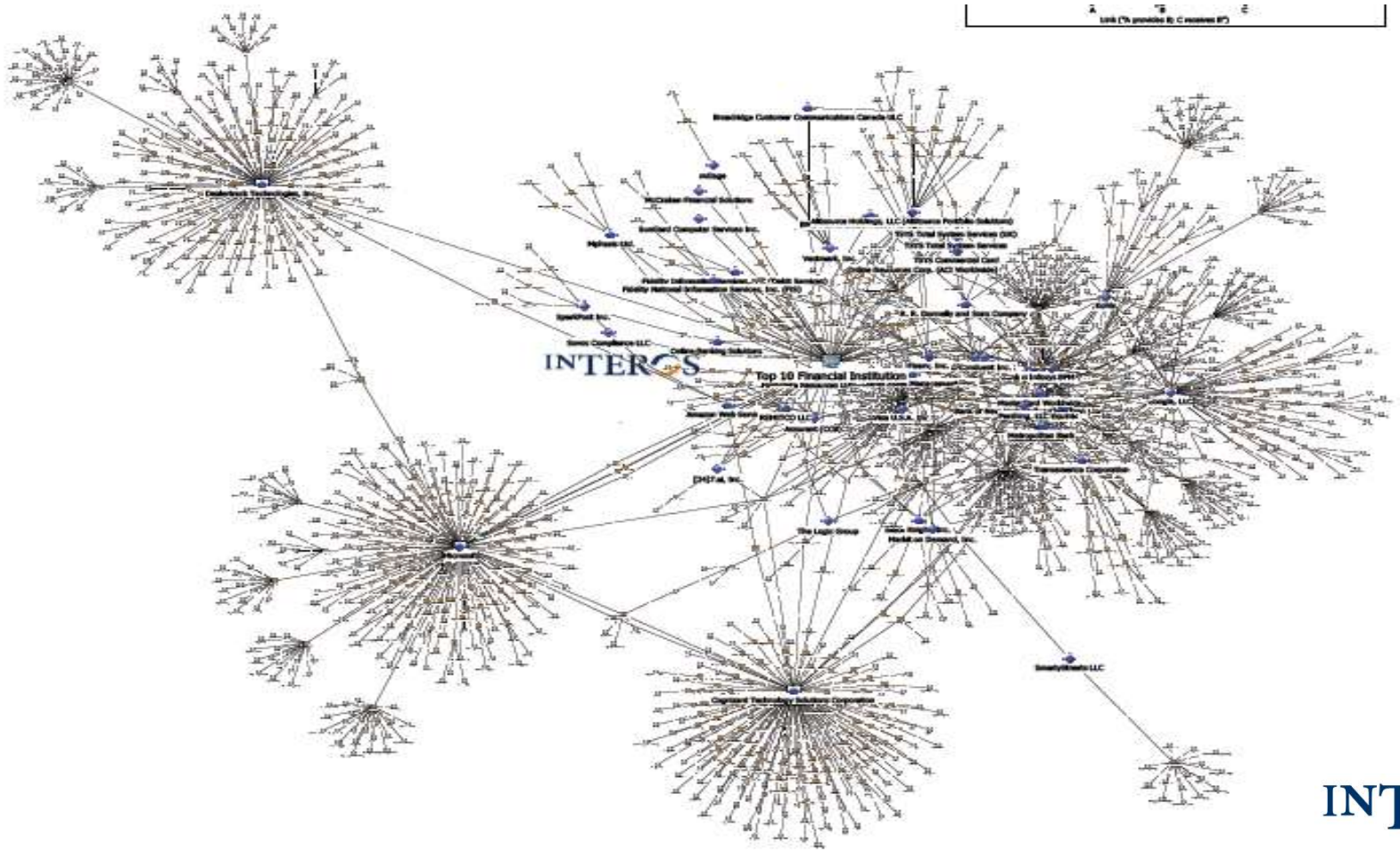
£1million per day
Losses after 900 KFC restaurants closed in the UK due to delivery failures

> $163B
Estimated counterfeit drug market

1,000's
Shipping containers trapped at Port of San Juan after Hurricane Maria

The networks of physical and digital supply chains are comprised of multi-tiered relationships that challenge transparency, risk management and resiliency.

Who is in your supply chain?



INTEROS

Cybersecurity threats to the supply chain

- Computer hardware delivered with malware installed
- Malware that is inserted into software or hardware post-delivery
- Software vulnerabilities in supply chain software applications
- Counterfeit computer hardware
- Loss of intellectual property shared with supply chain partners
- 3rd party access to IT networks, customer information or operational control systems
- Poor information security practices by lower-tier suppliers
- Rogue, malicious, or naïve inside employees

Bloomberg's Super Micro reporting

- China's intelligence services directed subcontractors to plant malicious chips in US company Super Micro motherboards
- The goal of hardware implants is to establish a covert staging area within sensitive networks and remotely access the compromised devices


Bloomberg the Company & Its Products | Bloomberg Anywhere Remote Login | Bloomberg Terminal Demo Request

Search

Bloomberg

Technology

New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom

The discovery shows that China continues to sabotage critical technology components bound for America.

By Jordan Robertson and Michael Riley

October 9, 2018, 11:01 AM EDT *Updated on October 9, 2018, 5:37 PM EDT*

- The Chinese infiltration through Super Micro reached almost 30 companies, including telecommunications providers, Amazon.com Inc. and Apple Inc.
- Super Micro stock plunged 41%

Super Micro, the USG, GCHQ, Amazon, Apple and everyone associated with the report have denied the existence of compromised hardware

Naval Undersea Warfare Center

- PLA Unit 61398 steals corporate trade secrets to benefit Chinese state-owned industry
- In early 2018, Chinese government hackers infiltrated the computers of a contractor working on a Navy submarine and underwater programs contract
- The hacked material includes 614GB of data on the Sea Dragon project, as well as signals and sensor data, submarine radio room information relating to cryptographic systems and the Navy submarine development unit's electronic warfare library

The Cost of NotPetya

In 2017, NotPetya malware spread from a Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations.

- Pharmaceutical company Merck - $870,000,000
- Delivery company FedEx (European subsidiary TNT Express) - $400,000,000
- French construction company Saint-Gobain - $384,000,000
- Danish shipping company Maersk - $300,000,000
- Snack company Mondelēz (parent of Nabisco and Cadbury) - $188,000,000
- British manufacturer Reckitt Benckiser - $129,000,000

The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Andy Greenberg in Wired, August 22, 2018

Maersk shipping corporate empire

- 574 offices
- 130 countries
- 76 ports around the globe
- 800 seafaring vessels
- 80,000 employees
- 20% of the entire world's shipping capacity

Dead in the water!

Committee on Foreign Investment in the U.S.

- CFIUS is an inter-agency committee authorized to review transactions, *including acquisitions of critical infrastructure,* that could result in control of a U.S. business by a foreign person and determine the impact of these transactions on national security
- Treasury Department leads, but multiple agencies get involved depending upon the company

"China has weaponized investment in an attempt to vacuum up our advanced technologies and simultaneously undermine our defense industrial base."

- Senator John Cornyn, February 13, 2018

CFIUS related activity

- Federal agencies banned from buying software from **Kaspersky Lab**, a Russian cybersecurity company, amid concerns about Russian spying.
- Chinese-backed investor, Canyon Bridge Capital Partners, has been blocked from buying **Lattice Semiconductor**, a California maker of highly programmable computer chips
- Chinese network equipment maker **Huawei**, which has been blocked from selling to U.S. phone companies amid spying concerns by federal officials
- Chinese drone giant **DJI**, which the Army reportedly banned amid security concerns
- Hong Kong's **TCL Industries**, which abandoned plans to buy the MiFi mobile Wi-Fi hotspot brand from San Diego's Inseego after regulatory scrutiny over security risks
- Hangzhou **Hikvision Digital Technology**, a large Hangzhou-based surveillance camera provider whose controlling shareholder is the Chinese government, has faced citizen complaints in the U.S. and U.K. over security concerns and its relationship with the Chinese government.

Cyber – supply chain's misguided brother

- 80% of all security breaches originate in the supply chain
- 45% of all cyber breaches attributed to past partners
- 72% of companies DO NOT have full visibility into their supply chains
- 59% of companies DO NOT have a process for assessing cybersecurity of third party providers with which they share data or networks
- 40% of attack campaigns targeted manufacturing and service sectors (20% each)

Jon Boyens, PM for SCRM at NIST, RSA Conference 2016

There is a > 0% chance your supply chain is already compromised

1. It's far more complicated than most people understand
2. Lack of formal contract agreements with 3rd parties
3. The cyber threat and vulnerability landscape is dynamic
4. Inconsistent application of information security standards and cyber hygiene in 3rd parties
5. n-tier suppliers have a different risk appetite than you

Findings from NIST Case Studies

- Existing tools to mitigate supply chain for quality, integrity, security and continuity risks *are also relevant for cyber risks*
- Best practices and tools to mitigate cyber risks in the supply chain are hiding in plain sight – often in other parts of the company

Synergies of solutions are not well exploited

Jon Boyens, PM for SCRM at NIST, RSA Conference 2016

What can you do?

- Know your vendors
  - Map your supply chain and identify your most important vendors
  - Identify your sub-tier suppliers with critical IT components or software embedded in your products and systems
  - Know, *WITHOUT A DOUBT*, what information or IT systems your vendors can access
  - Review your vendor personnel practices
- Ensure the CISO's team is integrated into the procurement process, vendor assessments and vendor management
- Conduct regular briefings on the threat environment and track the reporting and remediation of vulnerabilities

Interos* SCRM risk factor framework

REGULATORY AND LEGAL

Regulatory/legal trends, actions, issues, and financial concerns
USG contracts

PHYSICAL SECURITY

Evaluation of physical security across the supply chain, to include security issues and concerns emanating from people involved
the business/product

R&D INNOVATION

Investments and plans for production/process improvements and

BUSINESS ALLIANCES

Current state, strategy, and plans relative to key joint ventures, partnerships, acquisitions, etc.
concerns, company leaders, its associations, as well as person to person relationships

The challenges are growing . . .

Three technology trends are exacerbating cyber risks to supply chains

- IT-enabled Supply Chain Management - product and supply chain data run on top of business software that connects supply chains – and weak links abound globally
- Internet of Things (IoT) - everything is smart and interconnected
  - *The 'S' in IoT is for security*
- 3-D Printing - production is going viral and digital, and destroying the traditional supply chain

Jon Boyens, PM for SCRM at NIST, RSA Conference 2016

"If an organization doesn't understand which third parties have access to it's network and present the greatest risk to its data, it's digital ecosystem becomes a ticking time bomb just waiting to be exploited."

- Fred Kneip, CEO , CyberGRX

THE ENEMY ISN'T HACKERS IT'S APATHY

mark@varmour.com